

IRS: Don't Respond to Rebate E-mail Scam

Protect Your Identity

INDIANAPOLIS -The Internal Revenue Service wants you to know there may be a scam waiting in your e-mail inbox that looks very official but is dangerous to you and your computer.

"We're getting reports of people receiving an e-mail that appears to come from the IRS and tells recipients to respond to get their 2008 Economic Stimulus Refund," said Jodie Reynolds, IRS spokesperson for Indiana and Kentucky.

Reynolds says there are three things the IRS needs people to remember:

- The IRS never sends unsolicited e-mails about your taxes.
- If you get a scam e-mail, don't access any links or attachments.
- If you have filed a 2007 federal tax return with the IRS, you don't need to do anything else to get a stimulus payment. The IRS will take care of the rest.

According to Reynolds, if you have accessed a link or attachment in a scam e-mail, you may have allowed the scammer to download malicious software to your computer and you should immediately scan for viruses and spyware, plus be alert for suspicious activity on your financial accounts.

"If you have actually responded to a scam e-mail by giving out your private information," Reynolds said, "you should immediately take steps to prevent identity theft. You may now be a prime target."

"Taxpayers can help the IRS stop scammers by sending the original scam e-mail to the IRS at phishing@irs.gov. The e-mail must be forwarded using special instructions at IRS.gov or it loses the encoding needed to track it to its source," Reynolds said.

The IRS has received about 33,000 forwarded scam e-mails, reflecting more than a thousand different incidents. Investigations by the Treasury Inspector General for Tax Administration have identified host sites in numerous countries, including Argentina, Aruba, Australia, Austria, Canada, Chile, China, England, Germany, Indonesia, Italy, Japan, Korea, Malaysia, Mexico, Poland, Singapore and Slovakia, as well as the United States.

Reynolds also cautioned that scammers make contacts in various ways.

"While the IRS never sends unsolicited e-mails or text messages," she said, "we do frequently use the U.S. Mail and may even use a phone call or a visit to make contact with taxpayers. Scammers know this and may also use one of these methods to contact people."

The IRS usually already has information that includes your Social Security number, so it would be unusual for an IRS employee to ask for that. And if the person is asking for credit card, bank account or PIN numbers, that's a big red flag that it's not really the IRS contacting you.

If you have any doubt as to whether the person contacting you is really from the IRS, decline giving out any information until you have contacted the IRS toll-free at 1-800-829-1040 to confirm that it is a legitimate contact.

For more information about tax scams, visit www.irs.gov and check out the Dirty Dozen, a list of tax scams updated each year by the IRS. The IRS also provides information on its Web site to help taxpayers protect their personal and financial information. Just type Identity Theft in the key word search feature for additional information.